

(19) 世界知的所有権機関  
国際事務局



(43) 国際公開日  
2001年3月8日 (08.03.2001)

PCT

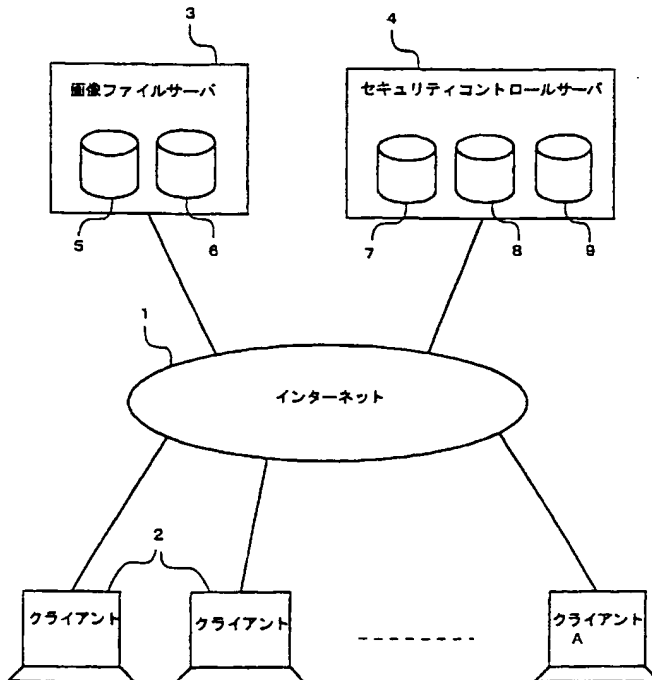
(10) 国際公開番号  
WO 01/17228 A1

- (51) 国際特許分類<sup>7</sup>: H04N 1/387, PUBLISHING JAPAN CO., LTD.) [JP/JP]; 〒603-8047 京都府京都市北区上賀茂本山196番地1号 Kyoto (JP).  
G06F 12/14, 15/00, G06T 1/00
- (21) 国際出願番号: PCT/JP00/05802 (72) 発明者; および  
(75) 発明者/出願人 (米国についてのみ): 新藤次郎 (SHINDO, Jiro) [JP/JP]; 〒603-8047 京都府京都市北区上賀茂本山196番地1号 株式会社 デジタル・パブリッシング・ジャパン内 Kyoto (JP).
- (22) 国際出願日: 2000年8月28日 (28.08.2000)
- (25) 国際出願の言語: 日本語
- (26) 国際公開の言語: 日本語 (74) 代理人: 梅田明彦(UMEDA, Akihiko); 〒107-0052 東京都港区赤坂3-6-10 第3セイコービル7F Tokyo (JP).
- (30) 優先権データ: 特願平11/283295, 1999年8月27日 (27.08.1999) JP (81) 指定国 (国内): CA, CN, JP, KR, US.
- (71) 出願人 (米国を除く全ての指定国について): 株式会社 デジタル・パブリッシング・ジャパン (DIGITAL (84) 指定国 (広域): ユーラシア特許 (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ特許 (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

[続葉有]

(54) Title: IMAGE DISTRIBUTING METHOD AND SYSTEM, IMAGE DATA, AND RECORDED MEDIUM

(54) 発明の名称: 画像データ配信方法及びシステム、画像データ並びに記録媒体



3...IMAGE FILE SERVER 2...CLIENT  
4...SECURITY CONTROL SERVER A...CLIENT  
1...INTERNET

(57) Abstract: An image distributing system comprises clients (2) connectable through a network environment such as the Internet (1), an image file server (3) having an image file database (5) where image files are stored and a log file (6), a user database (7), and a security control server (4) having an image key database (8) and a log file (9). A client who has requested an image makes an access to the security control server by means of an IP address that the client obtains from the image file server is authenticated, obtains an image key, can open image data from the image file server, encodes the security data including the date and time of the delivery of the image data, the user ID, the serial number of the hard disk, and the IP address of the client, buries the security data as electronic watermark in the image data developed on the own memory, sends the data to the security control server, and allows the server to store it in the log file.

[続葉有]



添付公開書類:

— 国際調査報告書

— 請求の範囲の補正の期限前の公開であり、補正審受領の際には再公開される。

2文字コード及び他の略語については、定期発行される各PCTガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

(57) 要約:

画像配信システムは、インターネット 1 などのようなネットワーク環境を通じて接続可能な複数のクライアント 2 と、画像ファイルを蓄積した画像ファイルデータベース 5 及びログファイル 6 を有する画像ファイルサーバ 3 と、ユーザデータベース 7、画像キーデータベース 8 及びログファイル 9 を有するセキュリティコントロールサーバ 4 とから構成される。画像を要求したクライアントが画像ファイルサーバから入手した IP アドレスでセキュリティコントロールサーバにアクセスし、認証を受けて画像キーを入手すると、画像ファイルサーバからの画像データを開くことができる。クライアントは、自己のメモリ上に展開した画像データに、画像データの配信日時、ユーザ ID、ハードディスクのシリアル番号、クライアントの IP アドレスなどのセキュリティデータを符号化して、電子透かしとして埋め込むと同時に、セキュリティコントロールサーバに送信してログファイルに保存させる。

## 明 細 書

### 画像データ配信方法及びシステム、画像データ並びに記録媒体

#### 技術分野

本発明は、デジタル化した画像をネットワークを介して配信するための技術に関し、特に配信した画像データの不正使用を防止・抑制するための画像データ配信方法及びシステム、並びにそれに使用される画像データに関する。

#### 背景技術

一般に、インターネットなどのネットワークを介して配信されるデジタル画像データは、画質を劣化させることなく容易に複製できるので、権限の無い者が無断で再配信したり複製するなど、不正使用される虞がある。このため、従来より、例えば特開平 9 - 1 9 1 3 9 4 号公報に記載されるように、配信する画像データに予め著作権や出所を示す情報を埋め込む電子透かし又はデジタル透かしという方法が開発されている。

ところが、このように著作権者などの出所を付加するだけの電子透かしでは、不正使用が判明した場合にも、そのデータが何時、どのクライアントに対し、どのアカウントに基づいて配信されたものかなど、流出したデータの配信ルートを特定することができないという問題があった。そこで、例えば特開 2 0 0 0 - 5 0 0 4 7 号公報などにおいて、配信相手先を特定する情報を予め画像データなどに埋め込んでおくデータ配信方法が提案されている。しかしながら、このデータ配信方法においても、実際にどのユーザによるのかを示す情報が含まれていないため、データの使用経路を確実に特定できない虞がある。

そこで、本発明の目的は、配信された画像データのユーザによる実際の使用状況をより確実に知ることができ、それにより不正使用の場合にも、その流出経路を容易に特定することができ、更に画像データの不正使用を有効に防止又は抑制することができる画像データ配信方法及びシステムを提供することにある。

### 発明の開示

本発明によれば、サーバ側からネットワークを介してクライアント側への画像データの配信において画像データの不正使用を防止するために、クライアント側において、サーバ側から配信された画像データをメモリ上に展開した後、展開した画像データにユーザのセキュリティデータを付加する過程とを含むことを特徴とする画像データ配信方法が提供される。

これにより、不正使用防止のためのユーザ又はクライアントの認識データであるセキュリティデータを、実際に画像データの配信を受けたクライアントにおいて、画像データ自体の内部に付加することができ、画像データが不正使用された場合にも、その使用経路を容易に追跡して特定することができる。そのため、画像データの不正利用に対して、従来よりも強い心理的抑制効果を発揮することができる。

或る実施例では、クライアント側からサーバ側にユーザのセキュリティデータを送信する過程と、該セキュリティデータをサーバ側の記憶装置に保存させる過程とを更に含むことにより、画像の不正使用があった場合には、画像データに付加されたセキュリティデータとサーバ側に保存されているセキュリティデータとを照合することができ、それにより画像データの使用経路をより確実に追跡し、特定することが可能である。

好ましくは、セキュリティデータを電子透かしとして画像データに付加することができる。

更に好ましくは、メモリ上に展開した前記画像データの各画素の中で連続しない位置にある複数の画素を選択し、選択した前記画素の輝度を増加又は減少させることにより、セキュリティデータを画像データに付加することができる。

また、本発明によれば、サーバ側からネットワークを介してクライアント側への画像データの配信において画像データの不正使用を防止するために、前記サーバ側において、クライアントからの要求に応答して、画像データ配信の認証を行うセキュリティコントローラへのアクセスを前記クライアント側に指示する過程と、前記クライアント側からの画像データ配信の認証要求に応答して、前記セキュリティコントローラから前記クライアント側に、画像データを開くための電

子キーを送信する過程とを含むことを特徴とする画像データ配信方法が提供される。

このように事前に配信相手先を認証することにより、画像データが権限の無い不正なユーザ又はクライアントに配信されることを防止することができる。

或る実施例では、クライアント側との通信状況を保存する過程を更に含むことにより、画像データの配信後に、その配信先をサーバ側で容易に確認できるので、不正使用があった場合にも、その使用経路をより容易に追跡し、特定することができる。

別の実施例では、画像データを配信するサーバとは別個にセキュリティコントローラを設け、そのIPアドレスをクライアント側に付与することにより、セキュリティコントローラへのアクセスを指示することが好ましい。

本発明の別の側面によれば、クライアント側又はサーバ側において、これらの画像データ配信方法を実行するためのソフトウェアを記憶した記録媒体が提供される。

本発明の更に別の側面によれば、サーバからクライアントへ画像データを配信するための方法であって、クライアント側からの画像データの要求に応答して、サーバ側から前記クライアント側にセキュリティコントローラへのアクセスを指示する過程と、前記クライアント側から前記セキュリティコントローラにアクセスして、画像データ配信の認証を求める過程と、前記サーバ側から前記クライアント側に前記要求に対応した画像データを送信する過程と、前記サーバ側から前記クライアント側に前記画像データを開くための画像キーを送信する過程と、前記クライアント側において、前記画像キーを用いて前記画像データを開き、該画像データにユーザのセキュリティデータを付加する過程と、前記セキュリティデータを付加した画像データを出力する過程とからなることを特徴とする画像データ配信方法が提供される。

このように構成することにより、事前に配信相手先を認証して、画像データが権限の無い不正なユーザ又はクライアントに配信されることを防止することができ、かつ、不正使用防止のためのユーザ又はクライアントの認識データであるセキュリティデータを、実際に画像データの配信を受けたクライアントにおいて

、画像データ自体の内部に付加できるので、画像データが不正使用された場合にも、その使用経路を容易に追跡して特定することができる。従って、従来よりも画像データの不正使用をより確実に防止することができ、かつ不正利用に対してより強い心理的抑止効果を発揮することができる。

或る実施例では、前記セキュリティデータをサーバ側に送信する過程と、該セキュリティデータをサーバ側において保存する過程とを更に含むことにより、画像の不正使用があった場合に、画像データに付加されたセキュリティデータとサーバ側に保存されているセキュリティデータとを照合して、画像データの使用経路をより確実に追跡し、特定することができる。

別の実施例では、サーバ側においてクライアント側との通信状況をログファイルに保存する過程を更に有することにより、不正使用のクライアント又はユーザを特定することがより一層確実にかつ容易になる。

また、或る実施例では、画像データを配信するサーバとは別個にセキュリティコントローラが設けられ、セキュリティコントローラへのアクセスを、そのIPアドレスをクライアント側に付与することにより指示することが好ましい。

別の実施例では、サーバ側から送信される画像データが圧縮されており、該画像データをクライアント側において解凍した後に、セキュリティデータを付加することができる。

また、セキュリティデータは、電子透かしとして画像データに付加することが好ましい。

或る実施例では、前記画像キーを用いて開いた画像データの各画素の中で連続しない位置にある複数の画素を選択し、選択した前記画素の輝度を増加又は減少させることにより、セキュリティデータを画像データに付加することができる。

セキュリティデータには、画像データの配信日時、ユーザID、画像データを保存したクライアントの記憶装置のシリアル番号、又はクライアントのIPアドレスを含むことができ、これらを用いると、画像データ配信後の使用経過を容易に特定することができる。

本発明の別の側面によれば、画像ファイルを蓄積した画像ファイルデータベースを有する画像ファイルサーバと、各ユーザの登録データを蓄積したユーザデー

データベース、及び各画像ファイルを開くための画像キーを蓄積した画像キーデータベースを有するセキュリティコントロールサーバと、クライアントと、画像ファイルサーバ、セキュリティコントロールサーバ及びクライアントを接続するネットワークとを備え、

画像ファイルサーバが、クライアントからの画像データの要求に応答して、該クライアントにセキュリティコントロールサーバへのアクセスを指示する機能と、要求された画像データをクライアントに送信する機能とを有し、

クライアントが、セキュリティコントロールサーバにアクセスして、ユーザの画像データ取得の認証を要求する機能を有し、

セキュリティコントロールサーバが、クライアントからの認証の要求に応答して、ユーザデータベースを確認してユーザに認証を付与し、要求された画像データの画像キーを画像キーデータベースから送信する機能を有し、

クライアントが更に、画像キーを用いて、受信した画像データを開き、かつ該画像データにユーザのセキュリティデータを付加する機能を有することを特徴とする画像データ配信システムが提供される。

このように構成することにより、事前に配信相手先を認証して画像データが権限の無い不正なユーザ又はクライアントに配信されることを防止し、かつ、ユーザ又はクライアントの認識データであるセキュリティデータを、画像データの配信を受けたクライアントにおいて画像データ自体の内部に付加することにより、画像データの使用経路を容易に追跡して特定することができ、従来よりも画像データの不正使用をより確実に防止しかつ心理的に抑止することができる画像データの配信方法を実現することができる。

或る実施例では、クライアントが、セキュリティデータをセキュリティコントロールサーバに送信する機能を更に有し、セキュリティコントロールサーバが、セキュリティデータを保存する機能を更に有することにより、後で画像データの中のセキュリティデータとセキュリティコントロールサーバに保存されているものとを照合することができる。

別の実施例では、セキュリティコントロールサーバが、クライアントとの通信状況を保存するためのログファイルを有することにより、画像データの配信状況

をより正確に把握することができる。

画像ファイルサーバは、セキュリティコントロールサーバへのアクセスをそのIPアドレスを付与することにより指示することが好ましい。

或る実施例では、画像ファイルサーバから送信される画像データが圧縮されており、クライアントが、受信した画像データを解凍し、かつその後にセキュリティデータを付加する。

クライアントは、セキュリティデータを電子透かしとして画像データに付加する機能を有することが好ましい。

また、セキュリティデータには、画像データの配信日時、ユーザID、画像データを保存したクライアントの記憶装置のシリアル番号、又はクライアントのIPアドレスが含まれると、画像データの使用経路を特定する上で好都合である。

更に、本発明の別の側面によれば、各ドットの画素データのマップからなり、その位置が連続していない複数の選択した画素について、その輝度を増加又は減少させることにより、ユーザの情報を埋め込んだことを特徴とする画像データが提供される。

#### 図面の簡単な説明

図1は、本発明による画像データ配信システムの好適な実施例を示す概略構成図である。

図2は、図1の画像データ配信システムにおいて画像データを配信する過程を示すフロー図である。

#### 発明を実施するための最良の形態

図1は、本発明による画像配信システムの好適な実施例であるインターネット上でのシステム構成を概略的に示している。本実施例の画像配信システムは、インターネット1のようなネットワーク環境を通じて接続可能な複数のクライアント2と、画像ファイルサーバ3と、セキュリティコントロールサーバ4とから構成される。クライアント2は、インターネット1上でWWWブラウザなどを用いて、画像ファイルサーバ3に所望の画像を指定した要求を送信し、該サーバか

らデジタル画像データを受信して画像を再生する機能を有するコンピュータである。

画像ファイルサーバ3は、インターネット上でクライアント2からの要求に応じて画像データを送信するコンピュータからなり、画像ファイルを蓄積した画像ファイルデータベース5と、クライアント2との通信状況を保持するログファイル6とを有する。更に画像ファイルサーバ3は、クライアント2から画像データの要求があると、これに応答してクライアント2にセキュリティコントロールサーバ4のIPアドレスを送信して、セキュリティコントロールサーバへのアクセスを指示する機能と、要求された画像データを画像ファイルデータベース5からクライアントに送信する機能とを有する。

本実施例では、デジタル化された画像データを、その各画素が有する情報の有意性（例えば輝度又は輝度変化）に基づいて階層化しかつ再構成したデータ構造を有し、かつ圧縮した階層化画像ファイルが画像ファイルデータベース5に蓄積されている。このような階層化画像ファイルは、例えば本願発明者による国際出願番号PCT/JP00/04472号明細書に記載される画像圧縮方法を用いて生成することができる。この階層化画像ファイルは、各画素の位置情報と輝度情報とから構成され、その階層によって画像の品質、即ち解像度、サイズが異なるので、クライアントは、画像の品質を指定して画像データを要求することができる。

セキュリティコントロールサーバ4は、画像ファイルデータベース5の画像ファイルを利用できるユーザの登録内容を蓄積したユーザデータベース7と、前記画像ファイルを開くために必要な画像キーを蓄積した画像キーデータベース8と、クライアント2との通信状況を保持するログファイル9とを有する。本実施例のユーザデータベース7には、各ユーザ及びその識別データがいくつかのグループに分類して登録され、各グループ毎に異なる権限が付与され、それにより例えば使用できる画像の品質、即ち画像の解像度、サイズなどが異なる。

クライアント2は、画像ファイルサーバ3からセキュリティコントロールサーバ4のIPアドレスを受信すると、これを用いてセキュリティコントロールサーバにアクセスし、画像データの取得についてその認証を要求する機能を有する。

この認証要求に対して、セキュリティコントロールサーバ4は、ユーザデータベース7を確認してユーザに認証を付与し、要求された画像データに固有の画像キーを画像キーデータベース8から送信する機能を有する。

クライアント2は更に、前記画像キーを用いて、画像ファイルサーバ3から受信した画像データを開いてメモリ上に展開し、かつこの画像データにユーザのセキュリティデータを付加する機能を有する。このセキュリティデータには、画像データの配信日時、ユーザID、画像データをダウンロードしたハードディスクなどの記憶装置のシリアル番号、クライアント2のIPアドレスなど、不正使用があった場合にその使用経路を追跡するのに有用なクライアント又はユーザの認識データが含まれる。

次に、図2を用いて本発明による画像配信方法の好適な実施例を説明する。先ず、クライアント2において汎用又は専用のWWWブラウザなどのプログラムを起動させ、インターネット1を介して画像ファイルサーバ3に接続する。クライアント2が、所望の画像のファイル名及び品質を指定した要求を送信する（ステップS1）と、画像ファイルサーバ3は、セキュリティコントロールサーバ4のIPアドレスを返信する（ステップS2）。クライアント2は、このIPアドレスを用いてセキュリティコントロールサーバ4にアクセスし、画像データの取得について認証を要求する（ステップS3）。この認証要求は、ユーザID、クライアントのIPアドレス、クライアントに固有のデータであるハードディスク装置のシリアル番号などを使用する。

セキュリティコントロールサーバ4は、ユーザデータベース7を参照してユーザIDなどの登録データを確認し、認証を与える（ステップS4）。そして、要求された画像データに固有の画像キーを画像キーデータベース8から取得して、クライアント2に送信する（ステップS5）と同時に、これらの通信状況をログファイル9に記録して保存する（ステップS6）。他方、画像ファイルサーバ3は、要求された画像データを画像ファイルデータベース5から取得してクライアント2に送信する（ステップS7）。画像ファイルサーバ3も同様にクライアント2との通信状況をログファイル6に記録して保存する。

クライアント2は、セキュリティコントロールサーバ4から受信した画像キー

を用いて、画像ファイルサーバ3から受信した画像データを開きかつ解凍し、画像を構成する各ドットの画素データのマップとしてメモリ上に展開する（ステップS8）。そして、展開した画像データの中に、セキュリティデータを符号化して付加する（ステップS9）。セキュリティデータの付加は、一般に電子透かしと呼ばれる手法を用いて行う。本実施例では、展開した前記画像データの各ドットの中で、連続しない位置にある複数の画素を選択し、選択した前記画素の輝度を増加又は減少させることにより、電子透かしを挿入することができる。選択する前記画素の位置は、予め設定しておくことができ、また画像の内容などによって変更することができる。

このようにしてセキュリティデータを付加した画像データは出力され（ステップS10）、クライアントのディスプレイに直接表示したり、画像ファイルとしてハードディスクなどの記憶装置や他の記憶媒体に格納したり、別の機器にオンラインで転送して、様々に利用することができる。これと同時に、クライアント2は、前記セキュリティデータをセキュリティコントロールサーバ4に送信し（ステップS11）、セキュリティコントロールサーバ4はこれをログファイル9に記録・保存する（ステップS12）。

これにより、画像データの配信記録がセキュリティコントロールサーバ4に残されるので、後で画像データの不正使用があった場合にも、画像データ自体に埋め込まれているセキュリティデータとの照合により、その使用経路を容易に特定することができる。また、本実施例では、画像ファイルサーバ3とセキュリティコントロールサーバ4とが別個に設けられているので、予めネットワーク上でセキュリティコントロールサーバ4のアドレスを決めておけば、画像ファイルサーバ3は必要に応じて任意のアドレスに設定しても、即ち画像ファイルデータベース5を任意のサーバに設置しても、クライアントから送信されるセキュリティデータを管理することができる。

本発明の別の実施例では、画像ファイルサーバ3とセキュリティコントロールサーバ4とを一体にして1つのサーバで構成することができる。この場合、セキュリティコントロールサーバ4へのアクセス及び画像キーの使用を省略することができる。即ち、クライアント2は最初にサーバに画像配信の認証を要求し、

これに応答してサーバがユーザデータベース 7 を参照して認証を与えた後、クライアント 2 が画像の配信を要求し、所望の画像データが送信されるようにすることができる。この場合にも、クライアントが画像データを開いてメモリ上に展開した後、上記実施例と同様にセキュリティデータを画像データに付加し、かつサーバに送信し、これをサーバがログファイルに保存することは言うまでもない。

また、別の実施例では、画像ファイルサーバ 3 から配信する画像データの中に予めセキュリティコントロールサーバ 4 の IP アドレスを書き込んでおくことができる。この場合、画像ファイルサーバ 3 は、クライアント 2 から画像データ配信の要求を受けると、要求された画像データを送信する。クライアント 2 は、受信した画像データから IP アドレスを読み取ってセキュリティコントロールサーバ 4 にアクセスし、認証を要求する。セキュリティコントロールサーバ 4 が認証して画像キーを送信すると、クライアント 2 は該画像キーを用いて画像データを開くことができるようになる。

以上、本発明の好適な実施例について詳細に説明したが、本発明は、当業者に明らかなように、その技術的範囲内において上記実施例に様々な変更や変形を加えて実施し得ることは明らかである。例えば、本発明は、上述したインターネット以外のネットワークについても同様に適用することができる。

## 請求の範囲

1. サーバ側からネットワークを介してクライアント側への画像データの配信において画像データの不正使用を防止するために、前記クライアント側において、前記サーバ側から配信された画像データをメモリ上に展開した後、展開した前記画像データにユーザのセキュリティデータを付加する過程とを含むことを特徴とする画像データ配信方法。
2. 前記クライアント側から前記サーバ側に前記ユーザのセキュリティデータを送信する過程と、前記セキュリティデータを前記サーバ側の記憶装置に保存させる過程とを更に含むことを特徴とする請求項 1 に記載の画像データ配信方法。
3. 前記セキュリティデータを電子透かしとして前記画像データに付加することを特徴とする請求項 1 又は 2 のいずれかに記載の画像データ配信方法。
4. メモリ上に展開した前記画像データの各画素の中で連続しない位置にある複数の画素を選択し、選択した前記画素の輝度を増加又は減少させることにより、前記セキュリティデータを前記画像データに付加することを特徴とする請求項 1 乃至 3 のいずれかに記載の画像データ配信方法。
5. サーバ側からネットワークを介してクライアント側への画像データの配信において画像データの不正使用を防止するために、前記サーバ側において、クライアントからの要求に応答して、画像データ配信の認証を行うセキュリティコントローラへのアクセスを前記クライアント側に指示する過程と、前記クライアント側からの画像データ配信の認証要求に応答して、前記セキュリティコントローラから前記クライアント側に、画像データを開くための電子キーを送信する過程とを含むことを特徴とする画像データ配信方法。
6. 前記クライアント側との通信状況を保存する過程を更に含むことを特徴とする請求項 5 に記載の画像データ配信方法。
7. 前記セキュリティコントローラの IP アドレスを付与することにより、前記セキュリティコントローラへのアクセスを指示することを特徴とする請求項 5 又は 6 に記載の画像データ配信方法。
8. 請求項 1 乃至 3、5 乃至 7 のいずれかに記載の画像データ配信方法を実行す

るためのソフトウェアを記憶した記録媒体。

9. サーバからクライアントへ画像データを配信するための方法であって、

クライアント側からの画像データの要求に応答して、サーバ側から前記クライアント側にセキュリティコントローラへのアクセスを指示する過程と、

前記クライアント側から前記セキュリティコントローラにアクセスして、画像データ配信の認証を求める過程と、

前記サーバ側から前記クライアント側に前記要求に対応した画像データを送信する過程と、

前記サーバ側から前記クライアント側に前記画像データを開くための画像キーを送信する過程と、

前記クライアント側において、前記画像キーを用いて前記画像データを開き、該画像データにユーザ又はクライアントのセキュリティデータを付加する過程と、

前記セキュリティデータを付加した画像データを出力する過程とからなることを特徴とする画像データ配信方法。

10. 前記セキュリティデータを前記サーバ側に送信する過程と、該セキュリティデータを前記サーバ側において保存する過程とを更に含むことを特徴とする請求項9に記載の画像データ配信方法。

11. 前記サーバ側において前記クライアント側との通信状況をログファイルに保存する過程を更に有することを特徴とする請求項9又は10に記載の画像データ配信方法。

12. 前記セキュリティコントローラのIPアドレスを付与することにより、前記セキュリティコントローラへのアクセスを指示することを特徴とする請求項9乃至11のいずれかに記載の画像データ配信方法。

13. 前記サーバ側から送信される前記画像データが圧縮されており、該画像データを前記クライアント側において解凍した後に、前記セキュリティデータを付加することを特徴とする請求項9乃至12のいずれかに記載の画像データ配信方法。

14. 前記セキュリティデータを電子透かしとして前記画像データに付加するこ

とを特徴とする請求項 9 乃至 13 のいずれかに記載の画像データ配信方法。

15. 前記画像キーを用いて開いた前記画像データの各画素の中で連続しない位置にある複数の画素を選択し、選択した前記画素の輝度を増加又は減少させることにより、前記セキュリティデータを前記画像データに付加することを特徴とする請求項 9 乃至 14 のいずれかに記載の画像データ配信方法。

16. 前記セキュリティデータには、前記画像データの配信日時、ユーザ ID、前記画像データを保存した前記クライアントの記憶装置のシリアル番号、又は前記クライアントの IP アドレスが含まれることを特徴とする請求項 9 乃至 15 のいずれかに記載の画像データ配信方法。

17. 画像ファイルを蓄積した画像ファイルデータベースを有する画像ファイルサーバと、

各ユーザの登録データを蓄積したユーザデータベースと、前記各画像ファイルを開くための画像キーを蓄積した画像キーデータベースとを有するセキュリティコントロールサーバと、

クライアントと、

前記画像ファイルサーバ、前記セキュリティコントロールサーバ及び前記クライアントを接続するネットワークとを備え、

前記画像ファイルサーバが、前記クライアントからの画像データの要求に応答して、前記クライアントに前記セキュリティコントロールサーバへのアクセスを指示する機能と、要求された画像データを前記クライアントに送信する機能とを有し、

前記クライアントが、前記セキュリティコントロールサーバにアクセスして、ユーザの前記画像データ取得の認証を要求する機能を有し、

前記セキュリティコントロールサーバが、前記クライアントからの認証の要求に応答して、前記ユーザデータベースを確認して前記ユーザに認証を付与し、前記画像キーデータベースから前記要求された画像データの画像キーを送信する機能を有し、

前記クライアントが更に、前記画像キーを用いて、受信した前記画像データを開き、かつ前記画像データに前記ユーザのセキュリティデータを付加する機能を

有することを特徴とする画像データ配信システム。

18. 前記クライアントが、前記セキュリティデータを前記セキュリティコントロールサーバに送信する機能を更に有し、前記セキュリティコントロールサーバが、前記セキュリティデータを保存する機能を更に有することを特徴とする請求項17に記載の画像データ配信システム。

19. 前記セキュリティコントロールサーバが、前記クライアントとの通信状況を保存するためのログファイルを有することを特徴とする請求項17又は18に記載の画像データ配信システム。

20. 前記画像ファイルサーバが、前記セキュリティコントロールサーバのIPアドレスを付与することにより、それへのアクセスを指示することを特徴とする請求項17乃至19のいずれかに記載の画像データ配信システム。

21. 前記画像ファイルサーバから送信される前記画像データが圧縮されており、前記クライアントが、受信した前記画像データを解凍し、かつその後に前記セキュリティデータを付加することを特徴とする請求項17乃至20のいずれかに記載の画像データ配信システム。

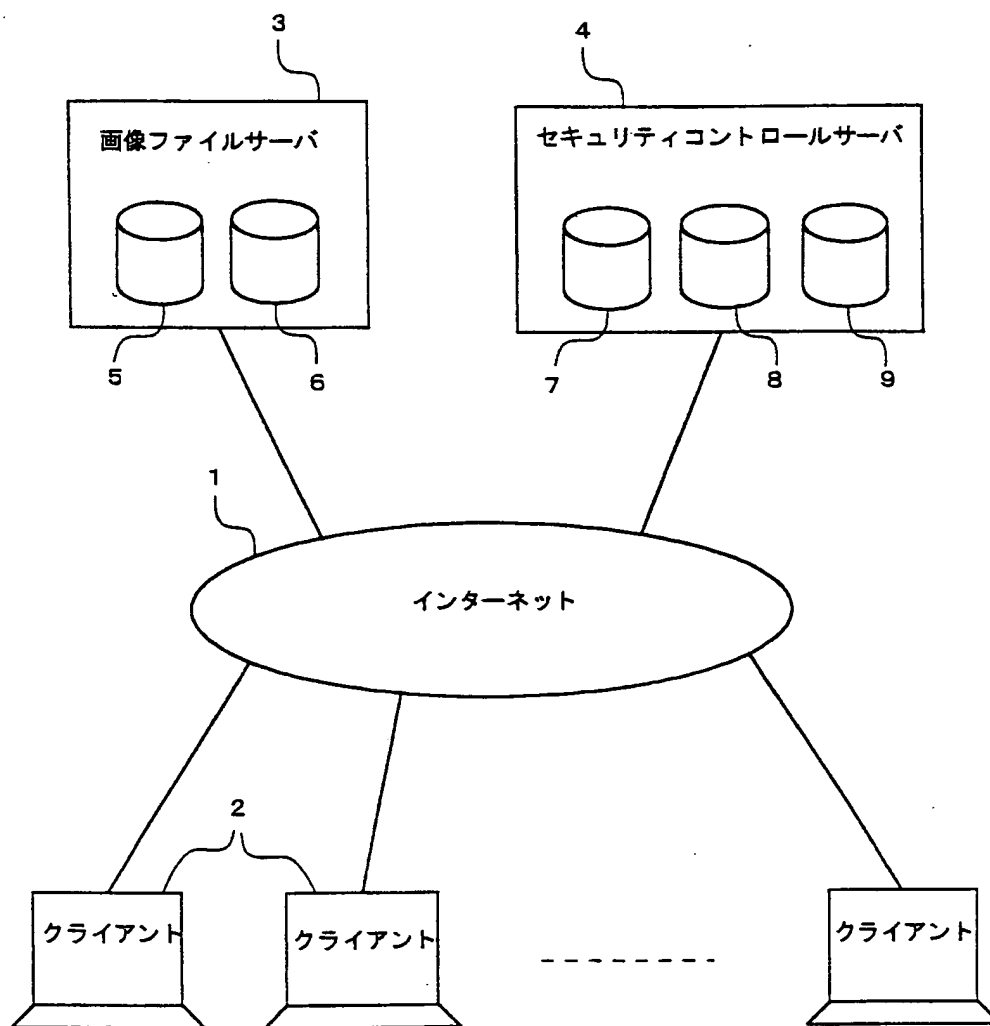
22. 前記クライアントが、前記セキュリティデータを電子透かしとして前記画像データに付加する機能を有することを特徴とする請求項17乃至21のいずれかに記載の画像データ配信システム。

23. 前記セキュリティデータには、前記画像データの配信日時、ユーザID、前記画像データを保存した前記クライアントの記憶装置のシリアル番号、又は前記クライアントのIPアドレスが含まれることを特徴とする請求項17乃至22のいずれかに記載の画像データ配信システム。

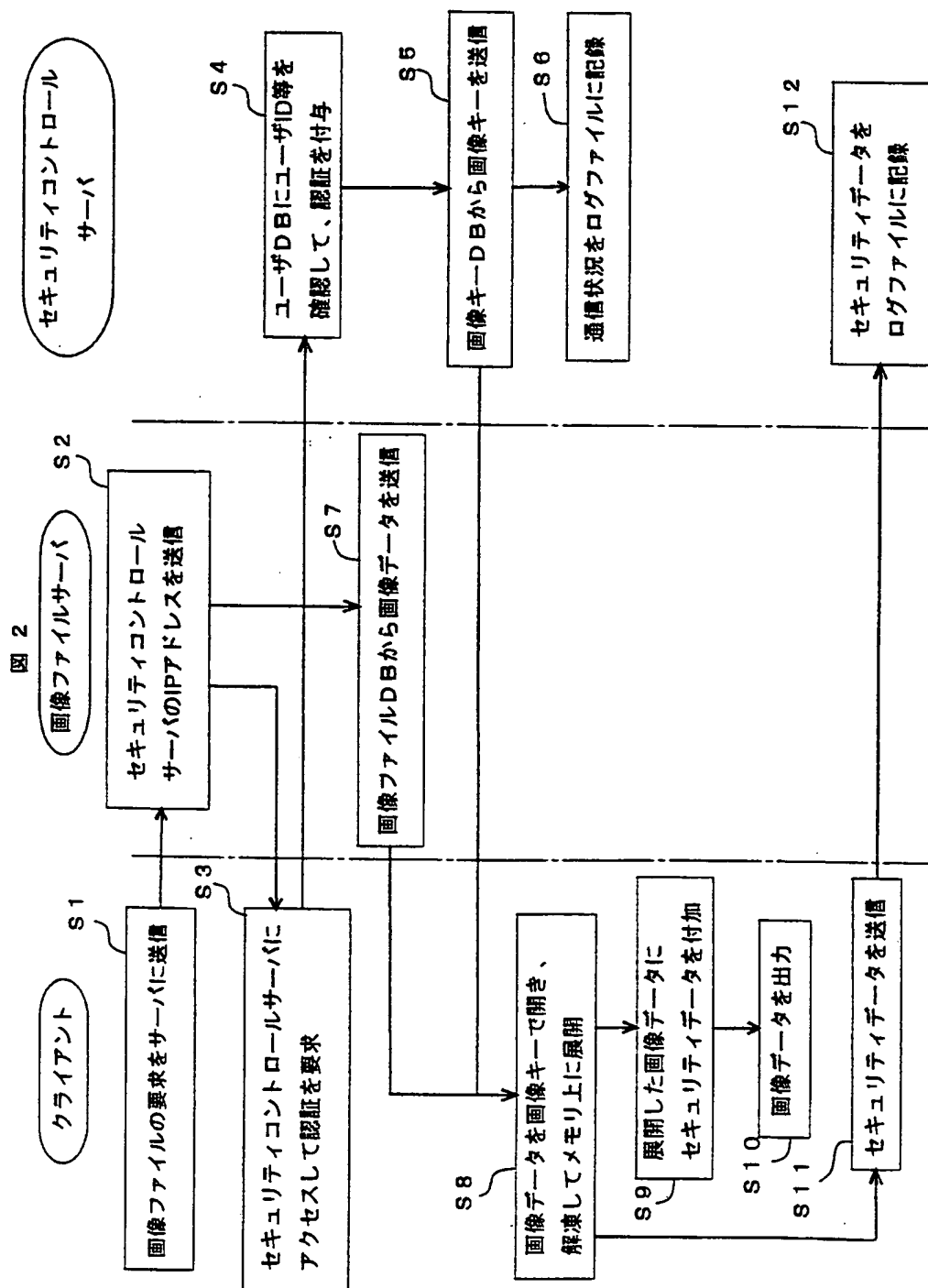
24. 各ドットの画素データのマップからなり、その位置が連続していない複数の選択した画素について、その輝度を増加又は減少させることにより、ユーザの情報を埋め込んだことを特徴とする画像データ。

1/2

図 1



2/2



# INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP00/05802

## A. CLASSIFICATION OF SUBJECT MATTER

Int.Cl<sup>7</sup> H04N1/387, G06F12/14, G06F15/00, G06T1/00

According to International Patent Classification (IPC) or to both national classification and IPC

## B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Int.Cl<sup>7</sup> H04N1/38-1/393, G06F12/14, G06F15/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho 1922-1996 Toroku Jitsuyo Shinan Koho 1994-2000  
Kokai Jitsuyo Shinan Koho 1971-2000 Jitsuyo Shinan Toroku Koho 1996-2000

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

## C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X Y	JP, 11-66010, A (Canon Inc.), 09 March, 1999 (09.03.99), Full text; Figs. 1 to 12 Full text; Figs. 1 to 12 & EP, 898396, A2	1-3, 5-14, 16 4, 15, 24
X Y	JP, 11-212461, A (Canon Inc.), 06 August, 1999 (06.08.99), Full text; Figs. 1 to 17 Full text; Figs. 1 to 17 (Family: none)	1-3, 5-14, 16 4, 15, 24
X Y	JP, 11-69137, A (Canon Inc.), 09 March, 1999 (09.03.99), Full text; Figs. 1 to 12 Full text; Figs. 1 to 12 & EP, 898396, A2	1-3, 5-14, 16 4, 15, 24
X Y	JP, 11-234264, A (Canon Inc.), 27 August, 1999 (27.08.99), Full text; Figs. 1 to 8 Full text; Figs. 1 to 8 (Family: none)	1-3, 5-14, 16 4, 15, 24

☒ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:	"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A" document defining the general state of the art which is not considered to be of particular relevance	"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E" earlier document but published on or after the international filing date	"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&" document member of the same patent family
"O" document referring to an oral disclosure, use, exhibition or other means	
"P" document published prior to the international filing date but later than the priority date claimed	

Date of the actual completion of the international search  
12 December, 2000 (12.12.00)

Date of mailing of the international search report  
26 December, 2000 (26.12.00)

Name and mailing address of the ISA/  
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

## INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP00/05802

## C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP, 11-69134, A (Sony Corporation), 09 March, 1999 (09.03.99), Full text; Figs. 1 to 13 (Family: none)	4, 15, 24
Y	JP, 9-252397, A (Tateba System K.K.), 22 September, 1997 (22.09.97), Full text; Figs. 1 to 3 (Family: none)	4, 15, 24
A	JP, 10-191036, A (Monorisu K.K.), 21 July, 1998 (21.07.98), Full text; Figs. 1 to 16 & WO, 98/20672, A2 & AU, 5430898, A & EP, 938807, A	1-24
A	JP, 10-285381, A (Matsushita Graphic Communication Systems, Inc.), 23 October, 1998 (23.10.98), Full text; Figs. 1 to 4 (Family: none)	1-24
A	JP, 11-203075, A (Canon Inc.), 30 July, 1999 (30.07.99), Full text; Figs. 1 to 5 (Family: none)	1-24

A. 発明の属する分野の分類 (国際特許分類 (IPC))		
Int. Cl <sup>7</sup> H04N1/387, G06F12/14, G06F15/00, G06T1/00		
B. 調査を行った分野		
調査を行った最小限資料 (国際特許分類 (IPC))		
Int. Cl <sup>7</sup> H04N1/38-1/393, G06F12/14, G06F15/00		
最小限資料以外の資料で調査を行った分野に含まれるもの		
日本国実用新案公報 1922-1996年 日本国公開実用新案公報 1971-2000年 日本国登録実用新案公報 1994-2000年 日本国実用新案登録公報 1996-2000年		
国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)		
C. 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
X Y	JP, 11-66010, A (キヤノン株式会社) 9. 3月. 1999 (09. 03. 99) 全文, 第1-12図 全文, 第1-12図 & EP, 898396, A2	1-3, 5-14, 16 4, 15, 24
X Y	JP, 11-212461, A (キヤノン株式会社) 6. 8月. 1999 (06. 08. 99) 全文, 第1-17図 全文, 第1-17図 (ファミリーなし)	1-3, 5-14, 16 4, 15, 24
<input checked="" type="checkbox"/> C欄の続きにも文献が列挙されている。 <input type="checkbox"/> パテントファミリーに関する別紙を参照。		
* 引用文献のカテゴリー 「A」 特に関連のある文献ではなく、一般的技術水準を示すもの 「E」 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの 「L」 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す) 「O」 口頭による開示、使用、展示等に言及する文献 「P」 国際出願日前で、かつ優先権の主張の基礎となる出願日の後に公表された文献 「T」 国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの 「X」 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの 「Y」 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの 「&」 同一パテントファミリー文献		
国際調査を完了した日 12. 12. 00		国際調査報告の発送日 26.12.00
国際調査機関の名称及びあて先 日本国特許庁 (ISA/JP) 郵便番号 100-8915 東京都千代田区霞が関三丁目4番3号		特許庁審査官 (権限のある職員) 橘爪 正樹 電話番号 03-3581-1101 内線 3571

C (続き) . 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
X Y	JP, 11-69137, A (キヤノン株式会社) 9. 3月. 1999 (09. 03. 99) 全文, 第1-12図 全文, 第1-12図 & EP, 898396, A2	1-3, 5-14, 16 4, 15, 24
X Y	JP, 11-234264, A (キヤノン株式会社) 27. 8月. 1999 (27. 08. 99) 全文, 第1-8図 全文, 第1-8図 (ファミリーなし)	1-3, 5-14, 16 4, 15, 24
Y	JP, 11-69134, A (ソニー株式会社) 9. 3月. 1999 (09. 03. 99) 全文, 第1-13図 (ファミリーなし)	4, 15, 24
Y	JP, 9-252397, A (立羽システム株式会社) 22. 9月. 1997 (22. 09. 97) 全文, 第1-3図 (ファミリーなし)	4, 15, 24
A	JP, 10-191036, A (株式会社モノリス) 21. 7月. 1998 (21. 07. 98) 全文, 第1-16図 & WO, 98/20672, A2 & AU, 5430898, A & EP, 938807, A	1-24
A	JP, 10-285381, A (松下電送システム株式会社) 23. 10月. 1998 (23. 10. 98) 全文, 第1-4図 (ファミリーなし)	1-24
A	JP, 11-203075, A (キヤノン株式会社) 30. 7月. 1999 (30. 07. 99) 全文, 第1-5図 (ファミリーなし)	1-24